AMENDMENTS TO CLAIMS

Please amend the claims as indicated.

1. (Currently Amended) A secure data processing device, the device configured as a Trusted Platform Module (TPM) and comprising:

a secure function module configured to receive an excluding computing module context, and to transact secure functions with an excluding computing module comprising storing cryptographic keys for the excluding computer module in which the secure function module receives the excluding computing module's context enabling the secure function module to transact the secure function with the excluding computing module;

the secure function module further configured to receive an non-conforming computing module context, and to transact secure functions with a non-conforming computing module comprising storing cryptographic keys for the non-conforming computing module in which the secure function module receives the non-conforming computing module's context enabling the secure function module to transact the secure function with the non-conforming computing module;

a communication module configured to communicate with the excluding computing module, the excluding computing module configured to exclusively transact the secure function with the secure function module, the communication module further configured to communicate with the non-conforming computing module, the non-conforming computing module configured to transact the secure function with the secure function module; and

a context module configured to either set the context of the secure function module to the excluding computing module context or~~and,~~ to set the context of the secure function module to non-conforming computing module context.

2. (Canceled)

3. (Canceled)

4. (Currently Amended) The device of claim 1, wherein context module is configured to arbitrate the setting of the context of the secure function module to either the excluding computing module context or ~~and~~ to the non-conforming computing module context.

5. (Original) The device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to an electrical signal.

6. (Previously Presented) The device of claim 5, wherein the electrical signal is an address.

7. (Original) The device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to data communicated to the communication module.

8. (Currently Amended) A computing module, the module comprising:

an identification module configured to identify an excluding computing module to a TPM ~~secure computing module~~ and set the context of the TPM ~~secure computing module~~ to an excluding computing module context enabling the TPM to transact a first secure function with the excluding computing module, the first

secure function comprising storing cryptographic keys for the excluding computing module;

the identification module further configured to identify a non-conforming computing module to the TPM~~secure computing module~~ and set the context of the secure computing module to a non-conforming computing module context enabling the TPM to transact a second secure function with the non-conforming computing module, the second secure function comprising storing cryptographic keys for the non-conforming computing module;

an address module configured to address a secure function of the TPM~~secure computing module~~; and

a data module configured to exchange data with the TPM~~secure computing module~~.

9. (Currently Amended) The module of claim 8, the identification module further configured to identify the excluding computing module and non-conforming computing module with an address communicated from the address module.

10. (Currently Amended) The module of claim 8, the identification module further configured to identify the excluding computing module and non-conforming computing module with data communicated from the data module.

11. (Currently Amended) A secure data processing system, the system comprising:

a TPM~~secure computing module~~ configured to identify a computing module responsive to the computing module initiating transacting a secure function with the TPM~~secure computing module~~, the TPM~~secure computing~~

~~module~~ further configured to set the context of the TPM~~secure computing module~~ to the computing module context enabling the TPM to transact the secure function with the computing module, wherein the TPM~~secure computing module~~ is configured to transact the secure function with the computing module, the secure function comprising storing cryptographic keys for the computing module;

an excluding computing module configured to initiate transacting the secure function with the TPM~~secure computing module~~, the excluding computing module further configured to exclusively transact the secure function with the TPM~~secure computing module~~; and

a non-conforming computing module configured to initiate transacting the secure function with the TPM~~secure computing module~~, the non-conforming computer module further configured to transact the secure function with the TPM~~secure computing module~~, wherein either the excluding computing module or the non-conforming computing module transacts the secure function with the TPM.

12. (Canceled)

13. (Canceled)

14. (Currently Amended) The system of claim 11, wherein the TPM~~secure computing module~~ identifies the excluding computing module and non-conforming computing module from an electrical signal.

15. (Original) The system of claim 14, wherein the electrical signal is an address.

16. (Currently Amended) The system of claim 11, wherein the TPM~~secure computing module~~ identifies the excluding computing module and non-conforming computing module from a data value.

17. (Currently Amended) A computer readable storage medium comprising computer readable code executable by a digital processing apparatus, the computer readable code configured to:

identify a computing module as an excluding computing module if the computing module is an excluding computing module;

identify the computing module as a non-conforming computing module if the computing module is a non-conforming computing module;

set a TPM~~secure computing module~~ to an excluding computing module context if the computing module is an excluding computing module enabling the TPM to transact a secure function with the excluding computing module and a non-conforming computing module context if the computing module is a non-conforming computing module enabling the TPM to transact the secure function with the non-conforming computing module; and

transact [[a]]the secure function comprising storing cryptographic keys between the TPM~~secure computing module~~ and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.

18. (Canceled)

19. (Currently Amended) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module as an ~~the computing module~~ initiatoring of the secure function transaction.

20. (Currently Amended) The computer readable storage medium of claim 17, further comprising computer readable code configured to arbitrate the setting of the context of the TPM~~secure computing module~~ between the excluding~~a first identified~~ computing module and the non-conforming~~a second identified~~ computing module.

21. (Currently Amended) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to an electrical signal.

22. (Currently Amended) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to an address.

23. (Currently Amended) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to a data value.

24. (Currently Amended) A secure computing method, the method comprising:

identifying a computing module as an excluding computing module if the computing module is an excluding computing module;

identifying the computing module as a non-conforming computing module if the computing module is a non-conforming computing module;

setting a TPM~~secure computing module~~ to an excluding computing module context enabling the TPM to transact a secure function with the excluding computing module if the computing module is an excluding module and a non-conforming computing module context enabling the TPM to transact the secure function with the non-conforming computing module if the computing module is a non-conforming computing module; and

transacting [[a]]the secure function comprising storing cryptographic keys between the TPM~~secure computing module~~ and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.

25. (Canceled)

26. (Original) The method of claim 24, further comprising initiating the transacting of the secure function.

27. (Currently Amended) The method of claim 24, further comprising arbitrating the setting of the TPM~~secure computing module~~ context between the excluding~~a first~~ computing module and the non-conforming~~a second~~ computing module.

28. (Currently Amended) The method of claim 24, wherein ~~the computing module is identified from~~ an electrical signal identifies the excluding computing module and the non-conforming computing module.

29. (Currently Amended) The method of claim 24, wherein ~~the computing module is identified from~~ a data value identifies the excluding computing module and the non-conforming computing module.

30. (Currently Amended) An apparatus for secure computing, the apparatus comprising:

means for identifying a computing module as an excluding computing module if the computing module is an excluding computing module;

means for identifying the computing module as a non-conforming computing module if the computing module is a non-conforming computing module;

means for setting a TPM~~secure computing module~~ to an excluding computing module context enabling the TPM to transact a secure function with the excluding computing module if the computing module is an excluding computing module and a non-conforming computing module context enabling the TPM to transact the secure function with the non-conforming computing module if the computing module is a non-conforming computing module; and

means for transacting [[a]]the secure function comprising storing cryptographic keys between the TPM~~secure computing module~~ and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.